

**IN THE UNITED STATES DISTRICT COURT FOR THE  
WESTERN DISTRICT OF PENNSYLVANIA**

In the Matter of the Application of the UNITED )  
STATES of America FOR AN ORDER )  
DIRECTING A PROVIDER OF )  
ELECTRONIC COMMUNICATIONS )  
SERVICE TO DISCLOSE RECORDS TO THE )  
GOVERNMENT, )

Magistrate's No. 07-524M

**BRIEF OF AMICI CURIAE THE ELECTRONIC FRONTIER FOUNDATION, THE  
AMERICAN CIVIL LIBERTIES UNION, THE ACLU-FOUNDATION OF  
PENNSYLVANIA, INC., AND THE CENTER FOR DEMOCRACY AND  
TECHNOLOGY IN OPPOSITION TO THE GOVERNMENT’S REQUEST FOR  
REVIEW**

## TABLE OF CONTENTS

TABLE OF AUTHORITIES .....	iii
CORPORATE DISCLOSURE STATEMENT.....	vi
I. INTRODUCTION .....	1
II. INTERESTS OF <i>AMICI</i> .....	1
III. LEGAL STANDARD .....	2
IV. SUMMARY OF ARGUMENT .....	3
V. ARGUMENT .....	4
A. The Stored Communications Act Requires the Government to Obtain at Least a D Order Before Seizing CSLI. ....	4
1. The Stored Communications Act Broadly Protects Any “Information Pertaining To a Subscriber” of an Electronic Communication Service Provider, Including Stored CSLI...5	5
2. The Stored Communications Act Protects Stored CSLI Regardless of Whether a Cell Phone Constitutes a “Tracking Device.” .....	7
3. Absent Stored Communications Act Protection, No Other Statute Would Require Any Evidentiary Showing to a Court Prior to the Government’s Seizure of Stored CSLI. ... .....	10
a. Rule 41 Does Not Independently Require Probable Cause for the Compelled Disclosure of Stored CSLI. ....	11
b. The “Tracking Device Statute,” 18 U.S.C. § 3117, Does Not Independently Require Probable Cause for the Compelled Disclosure of Stored CSLI. ....	11
c. The Wireless Communication and Public Safety Act Does Not Independently Require Probable Cause for the Compelled Disclosure of Stored CSLI. ....	12
d. CALEA’s Restriction Against the Use of Pen Registers for Cell Phone Tracking Does Not Independently Require Probable Cause for the Compelled Disclosure of Stored CSLI.....	13
B. The Stored Communications Act Permits the Court to Require a Probable Cause Warrant Rather than a D Order Prior to the Seizure of Stored CSLI. ....	14
1. The Plain Language of 18 U.S.C. § 2703(d) is Permissive and Does Not Require Issuance of an Order Upon a Showing of Specific and Articulable Facts. ....	14
2. The Doctrine of Constitutional Avoidance Requires That This Court Interpret 18 U.S.C. § 2703(d) as Permissive Because the Statute Otherwise Runs Afoul of the Fourth Amendment.....	17
C. The Fourth Amendment Protects Stored CSLI, Such That the Government Must Obtain a Rule 41 Warrant Rather Than a D Order Prior to its Seizure.....	18

1. Stored CSLI Reveals Details about the Interior of Homes, Purses and Pockets, All Protected Spaces Under the Fourth Amendment. ....	18
2. The Invasive “Dragnet” Surveillance Enabled by CSLI Requires At Least A Probable Cause Showing.....	24
3. Because a Reviewing Court Cannot Otherwise Ensure that The Disclosure of Stored CSLI Will Not Violate the Fourth Amendment, an Order Compelling the Disclosure of Such CSLI Should Only Issue If the Government Makes the Showing Required by Rule 41 .....	26
4. CSLI is a Third Party Record in Which the Subscriber Has a Reasonable Expectation of Privacy.....	29
VI. CONCLUSION.....	31

## TABLE OF AUTHORITIES

### Cases

<i>Ashwander v. Tennessee Valley Authority</i> , 297 U.S. 288 (1936).....	17
<i>Dendrite Intern., Inc. v. Doe No. 3</i> , 775 A.2d 756 (N.J. Super. Ct. App Div. 2001).....	28
<i>Doe v. Cahill</i> , 884 A.2d 451 (Del. 2005).....	28
<i>Duncan v. Walker</i> , 533 U.S. 167 (2001).....	15
<i>Haines v. Liggett Group Inc.</i> , 975 F.2d 81 (3rd Cir. 1992).....	2
<i>Highfields Capital Mgmt. L.P. v. Doe</i> , 385 F. Supp. 2d 969 (N.D. Cal. 2004).....	28
<i>Hoffa v. United States</i> , 385 U.S. 293 (1966).....	18, 22
<i>ICG Communications, Inc. v. Allegiance Telecom</i> , 211 F.R.D. 610 (N.D. Cal. 2002) .....	12
<i>In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority</i> , 396 F. Supp. 2d 747 (S.D. Tex. 2005).....	7, 8, 30
<i>In re Application of the United States for an Order (1) Authorizing the Use of a Pen Register &amp; a Trap &amp; Trace Device &amp; (2) Authorizing Release of Subscriber Info. &amp;/or Cell Site Info.</i> , 384 F. Supp. 2d 562 (E.D.N.Y. 2005).....	1
<i>In re Application of the United States for an Order (1) Authorizing the Use of a Pen Register &amp; a Trap &amp; Trace Device &amp; (2) Authorizing Release of Subscriber Info. &amp;/or Cell Site Info.</i> , 396 F. Supp. 2d 294 (E.D.N.Y. 2005).....	30
<i>In re Application of the United States of America for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace</i> , 405 F. Supp. 2d 435 (S.D.N.Y. 2005).....	6, 31
<i>In re Application of U.S. for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System</i> , 402 F. Supp. 2d 597 (D.M.D. 2005) .....	31
<i>In re Application of U.S. for an Order Authorizing use of A Pen Register and Trap On [XXX] Internet Service Account/User Name, [xxxxxxx@xxx.com]</i> , 396 F. Supp. 2d 45 (D.Mass. 2005) .....	16
<i>In re Application of U.S. for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; and (2) Authorizing Release of Subscriber Information and/or Cell Site Information</i> , 411 F. Supp. 2d 678 (W.D. La. 2006) .....	31
<i>In re Application of U.S. for Orders Authorizing the Installation and Use of Pen Registers and Caller Identification Devices</i> , 416 F. Supp. 2d 390 (D.Mass. 2005).....	31
<i>In re Application of U.S. for Orders Pursuant to Title 18, United States Code, Section 2703(d)</i> , 509 F. Supp. 2d 76 (D. Mass. 2007) .....	6, 31
<i>In re Doubleclick Inc. Privacy Litigation</i> , 154 F. Supp. 2d 497 (S.D.N.Y. 2001).....	28

<i>In re Government Application for Pen Register and Trap and Trace Device with Cell-Site Location Authority</i> , No. 06 Crim. Misc. 01 (S.D.N.Y. Dec. 6, 2005) .....	3
<i>In re: Application of the United States for an Order for Prospective Cell Site Location Information On a Certain Cellular Telephone</i> , 460 F. Supp. 2d 448 (2006).....	29
<i>In the Matter of an Application of the United States for an Order Authorizing the Use of a Pen Register and a Trap and Trace Device</i> , 396 F. Supp. 2d 294 (E.D.N.Y. 2005) .....	7
<i>In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government</i> , 534 F. Supp. 2d 585 (W.D. Pa. 2008).....	passim
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001) .....	passim
<i>Rosenberg v. XM Ventures</i> , 274 F.3d 137 (3d Cir. 2001).....	5
<i>Scott Paper Co. v. U.S.</i> , 943 F. Supp. 501 (E.D. Pa. 1996) .....	2
<i>SEC v. Jerry T. O'Brien, Inc.</i> , 467 U.S. 735 (1984) .....	29
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979) .....	29, 30, 31
<i>Tavarez v. Klingensmith</i> , 372 F.3d 188 (3rd Cir. 2004) .....	15
<i>United States v. Garcia</i> , 474 F.3d 994 (7th Cir. 2007).....	25
<i>United States v. Karo</i> , 468 U.S. 705 (1984).....	passim
<i>United States v. Knotts</i> , 460 U.S. 276 (1983).....	passim
<i>United States v. Leon</i> , 468 U.S. 897 (1984).....	28, 31
<i>United States v. Miller</i> , 425 U.S. 435 (1976) .....	10, 29
<i>Zadvydas v. Davis</i> , 533 U.S. 678 (2001).....	17
<b>Statutes</b>	
18 U.S.C. § 2510(12) .....	8, 9
18 U.S.C. § 2510(12)(c).....	8
18 U.S.C. § 2510(15) .....	6
18 U.S.C. § 2510(4) .....	9
18 U.S.C. § 2511.....	9
18 U.S.C. § 2518.....	9
18 U.S.C. § 2703(c)(1).....	passim
18 U.S.C. § 2703(c)(1)(a).....	14

18 U.S.C. § 2703(c)(2).....	5, 16
18 U.S.C. § 2707(c) .....	28
18 U.S.C. § 2708.....	28
18 U.S.C. § 3117(b).....	7
18 U.S.C. § 3123(a)(1).....	15
18 U.S.C. §§ 2701-12.....	4
18 U.S.C. §§ 3121-27.....	13
28 U.S.C. § 636(b)(1)(A) .....	2
47 U.S.C. § 1002(a)(1)(2) .....	13
47 U.S.C. § 222.....	12

## Rules

Federal Rule of Criminal Procedure 41 .....	passim
H.R. Rep. No. 103-827 (1994) .....	16, 17
H.R. Rep. No. 99-647 (1986) .....	17
S. Hrg. 98-1266 (1984) .....	10
S. Rep. No. 99-541 (1986) .....	10, 12

## Publications

Jennifer King & Chris Jay Hoofnagle, <i>Research Report: A Supermajority of Californians Supports Limits on Law Enforcement Access to Cell Phone Location Information</i> (April 18, 2008) .....	24
Pub. L. No. 103-414, Title II, § 207(a) (Oct. 25, 1994).....	16
Pub. L. No. 99-508, Title II, § 201 (Oct. 21, 1986).....	16
Wayne R. LaFave, <i>Search and Seizure: A Treatise on the Fourth Amendment</i> (4th ed. 2004)....	20

**CORPORATE DISCLOSURE STATEMENT**

Pursuant to Local Rule 7.1.1 of the Western District of Pennsylvania and to enable Judges and Magistrate Judges to evaluate possible disqualification or recusal, the undersigned counsel for *amici curiae* the Electronic Frontier Foundation (“EFF”), the American Civil Liberties Union (“ACLU”), ACLU-Foundation of Pennsylvania, Inc. (“ACLU of Pennsylvania”), and the Center for Democracy and Technology (“CDT”) certifies that *amici* are non-profit corporations with no parents, subsidiaries and/or affiliates that have issued shares or debt securities to the public.

Dated: July 31, 2008

\_\_\_\_\_/s/\_\_\_\_\_  
Jennifer Granick, Esq.  
Electronic Frontier Foundation  
454 Shotwell St.  
San Francisco, CA 94110

## I. INTRODUCTION

*Amici curiae* the Electronic Frontier Foundation (“EFF”), the American Civil Liberties Union (“ACLU”), the American Civil Liberties Union of Pennsylvania Foundation, Inc. (“ACLU of Pennsylvania”), and the Center for Democracy and Technology (“CDT”) respectfully urge this Court to affirm U.S. Magistrate Judge Lisa P. Lenihan’s February 19, 2008, denial of the government’s application for a court order under 18 U.S.C. § 2703(d) of the Stored Communications Act (“SCA”) to obtain stored cell site location information (“CSLI”) from a cellular telephone provider. *See In re the Application of the U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 534 F. Supp. 2d 585 (W.D. Pa. 2008) (“*M.J. Order*”). Magistrate Judge Lenihan correctly held that the SCA allows the Court to require the government to satisfy the requirements for the issuance of a Rule 41 warrant before authorizing the seizure of stored CSLI, *see id.* at 607-10, and that the Fourth Amendment requires the court to do so. *See id.* at 611-12.

## II. INTERESTS OF *AMICI*

The Electronic Frontier Foundation (“EFF”) is a member-supported, non-profit legal foundation that litigates to protect free speech and privacy rights in the digital world. As part of its mission, EFF has often served as counsel or *amicus* in key cases addressing the electronic surveillance statutes at issue here, including serving as *amicus* to Magistrate Judge Michael L. Orenstein, the first federal magistrate to publish an order denying a government application to track a cell phone’s location in real time without probable cause.<sup>1</sup>

The American Civil Liberties Union (“ACLU”) is a nationwide, nonprofit, nonpartisan organization with over 500,000 members dedicated to the principles of liberty and equality

---

<sup>1</sup> *See generally In re Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info.*, 384 F. Supp. 2d 562 (E.D.N.Y. 2005) (“*Orenstein I*”) (denying application); *In re Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info.*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005) (“*Orenstein II*”) (on reconsideration, reaffirming denial of application on alternate reasoning consistent with EFF’s *amicus* briefing).



embodied in the U.S. Constitution. The protection of privacy as guaranteed by the Fourth Amendment is an area of special concern to the ACLU. In this connection, the ACLU has been at the forefront of numerous state and federal cases addressing the right of privacy in Internet communications.

The ACLU-Foundation of Pennsylvania, Inc. (“ACLU of Pennsylvania”) is a non-profit organization with about 19,000 members in Pennsylvania. The organization is devoted to the preservation and advancement of civil liberties for all Pennsylvanians through public education, legislative advocacy and litigation. The ACLU of Pennsylvania regularly appears in this Court and the Third Circuit as either direct counsel or amicus to serve those ends. Because of its particular commitment to rights of privacy and due process, the ACLU of Pennsylvania has a special interest in, and expertise to address, the application of the law in this case.

The Center for Democracy and Technology (“CDT”) is a non-profit public interest organization focused on privacy and other civil liberties issues affecting the Internet and other communications networks. CDT represents the public’s interest in an open, decentralized Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

This *amicus* brief is submitted at the request and by the order of this Court, under its Briefing Order dated May 2, 2008, as amended.

### **III. LEGAL STANDARD**

The District Court may reconsider any non-dispositive magistrate order if it is shown that the order is clearly erroneous or contrary to law. 28 U.S.C. § 636(b)(1)(A). *See also, e.g., Haines v. Liggett Group Inc.*, 975 F.2d 81, 91 (3rd Cir. 1992) (noting that magistrate judge discovery orders under 28 U.S.C. § 636(b)(1)(A) are subject to a clearly erroneous standard); *Scott Paper Co. v. U.S.*, 943 F. Supp. 501, 502 (E.D. Pa. 1996) (“The Court may overrule a decision of the Magistrate Judge involving a nondispositive discovery dispute only if the decision is clearly erroneous or contrary to law, or if the Magistrate Judge abused his discretion.”).

#### IV. SUMMARY OF ARGUMENT

Three questions, laid out below, are material to resolving the government's application for stored CSLI. *Amici* respectfully disagree with Magistrate Judge Lenihan, and agree with the Department of Justice, on the answer to the first question. However, *amici* and Magistrate Judge Lenihan arrive at the same answers to the two remaining questions, and thus arrive at the same ultimate conclusion: that the Court can and must require the government to meet the requirements to obtain a Rule 41 warrant before issuing an order compelling the disclosure of stored CSLI.<sup>2</sup> The three questions, addressed in the three subsections of argument and answered by *amici* in the affirmative, are:

**First**, does the SCA protect stored CSLI as “a record or other information pertaining to a subscriber to or customer of” a “provider of electronic communication service” under 18 U.S.C. § 2703(c)(1), such that the statute requires the government to obtain *at least* a court order under 18 U.S.C. § 2703(d) (a “D Order”) before seizing it? *Amici*, agreeing with the government and disagreeing with Magistrate Judge Lenihan,<sup>3</sup> will show that the SCA does indeed protect stored CSLI.

**Second**, does the SCA permit the Court to require that the government obtain a warrant rather than a D Order prior to the seizure of stored CSLI? *Amici*, agreeing with Magistrate Judge Lenihan and disagreeing with the government,<sup>4</sup> will demonstrate that the “specific and articulable facts” showing required by Section 2703(d) is a necessary but not always sufficient condition for the issuance of a D Order, and that the Court in its discretion may accommodate

---

<sup>2</sup> *Amici* do not address the distinct issue of government acquisition of CSLI prospectively or in real time. See *Government's Memorandum of Law in Support of Request for Review* (“Gov. Br.”) at 10 n.6. However, for a summary of *amicus* EFF's position on that issue, i.e., that CSLI is not available prospectively without at least a Rule 41 warrant, see generally *Letter Brief of Amicus Curiae the Federal Defenders of New York and EFF to Chief Magistrate Judge Peck In re Government Application for Pen Register and Trap and Trace Device with Cell-Site Location Authority*, No. 06 Crim. Misc. 01 (S.D.N.Y. Dec. 6, 2005) (available at [http://www.eff.org/files/filenode/celltracking/EFF\\_FDNY\\_reply\\_brief.pdf](http://www.eff.org/files/filenode/celltracking/EFF_FDNY_reply_brief.pdf)).

<sup>3</sup> See Gov. Br. at 6-7. *But see M.J. Order*, 534 F. Supp. 2d at 604-07.

<sup>4</sup> See *M.J. Order*, 534 F. Supp. 2d at 607-09. *But see* Gov. Br. at 18-19.

privacy concerns associated with especially revealing information such as CSLI, and avoid raising serious constitutional doubts about the SCA's validity, by instead requiring that the government obtain a warrant under Federal Rule of Criminal Procedure 41 ("Rule 41 warrant").

**Third**, does the Fourth Amendment protect stored CSLI, such that the government must obtain a Rule 41 warrant rather than a D Order prior to its seizure? Although the doctrine of constitutional avoidance does not require the Court to reach this issue, *amici* will nevertheless show that the Fourth Amendment does indeed protect stored CSLI, agreeing with Magistrate Judge Lenihan that such data necessarily reveals information about Fourth Amendment-protected spaces such one's home, purse, or pocket.<sup>5</sup>

In sum, the SCA's statutory privacy protections for information pertaining to an electronic communication service provider's ("ECSP") customer certainly apply to stored CSLI. The SCA thereby sets a statutory *floor* of protection for stored CSLI by requiring that the government obtain *at least* a D Order based on "specific and articulable facts" before seizing it. However, as Magistrate Judge Lenihan correctly held, the Court may in its discretion raise that floor and require a warrant, and indeed must do so in this case, where to do otherwise would raise serious Fourth Amendment questions.

## V. ARGUMENT

### A. The Stored Communications Act Requires the Government to Obtain at Least a D Order Before Seizing CSLI.

Cell site location information stored by a cell phone provider is protected against government access by the Stored Communications Act ("SCA") portion of the Electronic Communications Privacy Act ("ECPA"),<sup>6</sup> which comprehensively regulates the disclosure of communications content, records and other information stored by electronic communication service providers. In particular, stored CSLI is protected under 18 U.S.C. § 2703(c)(1) of the

---

<sup>5</sup> See *M.J. Order*, 534 F. Supp. 2d at 610-16. *But* see Gov. Br. at 19-27.

<sup>6</sup> 18 U.S.C. §§ 2701-12.

SCA, which requires the government to obtain either a Rule 41 warrant or a D Order before seizing such information.

“Every exercise of statutory interpretation begins with an examination of the plain language of the statute,” and where statutory language is “plain and unambiguous,” no further inquiry is necessary. *Rosenberg v. XM Ventures*, 274 F.3d 137, 141 (3d Cir. 2001). The language of 18 U.S.C. § 2703(c)(1) plainly and unambiguously protects stored CSLI against seizure by the government absent a warrant or D Order. In relevant part, that provision states:

A governmental entity may require a provider of electronic communication service...to disclose *a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)* only when the governmental entity—

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;

(B) obtains a court order for such disclosure under subsection (d) of this section;

[or]

(E) seeks information under paragraph (2).

18 U.S.C. § 2703(c)(1) (emphasis added). In other words, the government has only three relevant options for compelling the disclosure of any non-content information pertaining to a customer of an ECSP: it can seek to obtain a Rule 41 warrant, it can seek to obtain a D Order, or, in certain limited instances not applicable here, it can seek to obtain with a subpoena information under paragraph (2) — so-called “subscriber information” such as name, address, and credit card information. *See* 18 U.S.C. § 2703(c)(2).

**1. The Stored Communications Act Broadly Protects Any “Information Pertaining To a Subscriber” of an Electronic Communication Service Provider, Including Stored CSLI.**

The government here seeks to compel cell phone provider Sprint Spectrum’s disclosure of “transactional records” regarding a specific subscriber’s cell phone account, including “historical cellular tower data” and “cellular tower site information.” *M.J. Order*, 534 F. Supp. 2d at 588. As an initial matter, there appears to be no disagreement between Magistrate Judge

Lenihan, the government, or *amici* about the meaning or applicability of several of 18 U.S.C. § 2703(c)(1)'s key terms in regard to these facts: Sprint Spectrum is a provider of an “electronic communication service” as that term is defined at 18 U.S.C. § 2510(15), by virtue of providing users the ability to send and receive wire communications such as phone calls and electronic communications such as text messages. *See* Gov. Br. at 6. The holder of the Sprint Spectrum account specified in the government's application is by definition a “customer of or subscriber to” Sprint Spectrum's service; and the stored CSLI sought by the government is “a record or other information” that is not “the contents of communications.” Rather, the controversy over the applicability of 18 U.S.C. § 2703(c)(1) to stored CSLI hinges solely on the meaning of the word “pertaining.” *See M.J. Order*, 534 F. Supp. 2d at 604 (holding that the location information derived from a cell phone “does not ‘pertain’ to the subscriber of an electronic communications service”).

*Amici* agree with the government that stored CSLI such as that at issue here — data that is routinely generated and recorded by the cell phone service provider in the ordinary course of providing communications service to its customer — “pertains” to that customer. *See* Gov. Br. at 5-8. *Amici* further agree with those many courts that, upon examining the same statutory language, have reached the same conclusion, such as Judge Stearns in the District Court of Massachusetts:

[T]he court must determine whether historical cell site information is “a record or other information pertaining to a subscriber to or customer of” an electronic communications service. ... Since neither the term “record” nor the term “information” is defined by the SCA, a court must look to the meaning of the terms in their ordinary usage. In the relevant context, a record means something stored or archived. The term information is synonymous with data. Cell phone service providers store data gleaned from the cell towers through which [a customer's] telephone calls are routed. Thus, historical cell site information is a “record or other information pertaining to” a customer....

*In re Application of U.S. for Orders Pursuant to Title 18, United States Code, Section 2703(d)*, 509 F. Supp. 2d 76, 79-80 (D. Mass. 2007) (“*Stearns*”) (internal citation omitted).<sup>7</sup>

---

<sup>7</sup> *See also, e.g., In re Application of the United States of America for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace*, 405 F. Supp. 2d 435, 445 (S.D.N.Y. 2005) (“*Gorenstein*”) (“It is certainly the case that cell site

**2. The Stored Communications Act Protects Stored CSLI Regardless of Whether a Cell Phone Constitutes a “Tracking Device.”**

Magistrate Judge Lenihan and the government disagree over whether a cell phone constitutes a “tracking device” as that term is broadly defined at 18 U.S.C. § 3117(b) (“an electronic or mechanical device which permits the tracking of the movement of a person or object”). *See M.J. Order*, 534 F. Supp. 2d at 602 (holding that cell phones are tracking devices), Gov. Br. at 13-17 (arguing that cell phones are not tracking devices). *Amici* take no position on this question, however, because its answer is irrelevant: even assuming that cell phones are tracking devices, the SCA would still protect stored CSLI as information pertaining to a customer under the plain language of 18 U.S.C. § 2703(c)(1), and would still require the government to obtain at least a D Order before seizing it.

*Amici* accept, for the sake of argument, that a cell phone may constitute a tracking device.<sup>8</sup> *See M.J. Order*, 534 F. Supp. 2d at 602 (asserting that it is “extremely difficult to see

---

or tracking information constitutes ‘information’ pertaining to customers or users of electronic communications services.”); *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747, 759 n.16 (S.D. Tex. 2005) (“*Smith*”) (“[H]istorical cell site data more comfortably fits the category of transactional records covered by the SCA.”); *In re Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device*, 2007 WL 3036849, \*4 (S.D. Tex. 2007) (holding that stored CSLI is a “‘a record or other information pertaining to a subscriber to or customer of’ an electronic communications service.”); *In the Matter of an Application of the United States for an Order Authorizing the Use of a Pen Register and a Trap and Trace Device*, 396 F. Supp. 2d 294, 303 n.6 (E.D.N.Y. 2005) (“If the government were seeking only historical cell site information, [the government’s position that a D Order authorized it to obtain CSLI] would of course be correct (though of course in such circumstances there would be no issue to resolve, as § 2703(d) plainly allows such relief).”).

<sup>8</sup> Even if true, “text messages or e-mail transmitted from [cell phones] could still be ‘electronic communications’” and therefore would not be protected from interception by the Wiretap Act, contrary to the government’s view. Gov. Br. at 16. As Magistrate Judge Smith in the Western District of Texas has explained:

This argument rests on a fallacy - i.e., that classifying cell site data as tracking information means that a cell phone must be regarded solely as a tracking device for all purposes, so that any form of communication from a cell phone *ipso facto* becomes a communication from a tracking device. Such reasoning ignores the multi-functional nature of the modern cell phone. ... Congress has decreed the highest protection for the contents of live conversations acquired via wiretap, intermediate protection for stored electronic communications, and the least

how a cell phone is not now *precisely* an ‘electronic...device which permits the tracking of the movement of a person or object.’”). *Amici* further accept *arguendo* that CSLI is excluded from the definition of an “electronic communication” under 18 U.S.C. § 2510(12)(c) (excluding from the definition “any communication from a tracking device (as defined in section 3117 of this title”). *See M.J. Order*, 534 F. Supp. 2d at 603. The exclusion of CSLI from the “electronic communication” definition does not, however, lead to CSLI’s complete “exclusio[n] from the ECPA (including the SCA),” and does not leave that information “set aside from” the SCA and “[outside] the scope” of 18 U.S.C. § 2703’s comprehensive protections. *M.J. Order*, 534 F. Supp. 2d at 604. Even if Congress intended the tracking device exclusion to protect CSLI in some way, that conclusion still cannot override the plain language of Section 2703(c)(1), which broadly covers any non-content information pertaining to the customer of an ECSP.

There is one obvious reason for the exclusion of tracking devices from the “electronic communication” definition, and it is not a privacy-protective one: pursuant to section 3117, when law enforcement seeks to intercept communications from a tracking device, it need not obtain an interception order under the Wiretap Act’s strict requirements.

Prior to ECPA’s passage, the Supreme Court had held that such government use of a tracking device could be authorized with only a regular search warrant, and in some cases may not require court approval at all. *See generally United States v. Knotts*, 460 U.S. 276 (1983) (monitoring of a tracking “beeper,” when such monitoring only reveals information that could have been derived from visual surveillance in public, does not implicate the Fourth Amendment

---

protection for telephone numbers dialed. The legal threshold for each type of communication is different, notwithstanding that a cell phone transmits them all. It would surely make no sense to impose the wiretap requirements upon a pen/trap application merely because the cell phone can be used to intercept live conversations; it makes no more sense to impose the tracking device requirements for access to other types of cell phone communications unrelated to physical location.

*Smith*, 396 F. Supp. 2d 747, 756 (S.D. Tex. 2005). As the government itself admits, such an “expansive interpretation” of the tracking device language would be senseless: “This result is plainly contrary to Congress’s purposes in passing ECPA....” Gov. Br. at 16.



nor require a warrant); *United States v. Karo*, 468 U.S. 705 (1984) (monitoring of tracking “beeper,” when such monitoring reveals information not exposed to the public, does implicate the Fourth Amendment and require a warrant). And although the broad statutory definition of “tracking device” is not so limited, Congress clearly intended it to at least apply to such tracking “beepers” as were used in *Karo* and *Knotts*:

*[Tracking devices] are one-way radio communication devices that emit a signal on a specific radio frequency. This signal can be received by special tracking equipment, and allows the user to trace the geographical location of the transponder. Such 'homing' devices are used by law enforcement personnel to keep track of the physical whereabouts of the sending unit, which might be placed in an automobile, on a person, or in some other item.*

S. Rep. 99-541 at 10 (emphasis added); *compare Knotts*, 460 U.S. at 277 (“A beeper is a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver.”).

Without the tracking device exclusion, the information transmitted by the government-installed tracking device described in the legislative history — the “signal” “emit[ted]” by this “communication device” — would appear to constitute an “electronic communication” protected against interception under the Wiretap Act. *See* 18 U.S.C. § 2510(12) (defining an “electronic communication” as “any transfer of signs, *signals*, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, *radio*, electromagnetic, photoelectronic or photooptical system....”) (emphasis added). Put another way, the government’s use of its “special tracking equipment” to receive the signal communicated from the tracking device would constitute an “intercept” of that communication, i.e., the “acquisition of the contents of any...electronic...communication through the use of any...device,” *id.* at § 2510(4), such that the government would have to first obtain an order under the Wiretap Act before engaging in such conduct. *See id.* at § 2511 (generally prohibiting interceptions), § 2518 (describing requirements for court orders authorizing interception). Excluding tracking device communications from the “electronic communication” definition avoids this result, consistent with *Karo* and *Knotts*. *See*,



e.g., S. Rep. 99-541 at 34 (noting that ECPA's treatment of tracking devices "does not effect current legal standards for the issuance" of court orders for the installation of tracking devices).

**3. Absent Stored Communications Act Protection, No Other Statute Would Require Any Evidentiary Showing to a Court Prior to the Government's Seizure of Stored CSLI.**

The SCA provides a statutory *restriction* on the government's ability to obtain information from ECSPs, protecting information that the government might otherwise obtain via voluntary disclosures or compel via mere subpoena. As such, it provides a statutory bulwark against government invasion into sensitive communications data, by imposing minimum privacy protection standards where Fourth Amendment protections are uncertain or unavailable.<sup>9</sup> Absent such protection, no significant statutory protection may exist. As outlined below, no statute or rule cited by the Court, either individually or taken together, requires the government to obtain a warrant to obtain stored CSLI.

---

<sup>9</sup> As the Senate Judiciary Committee's report on ECPA explained:

With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information. ... *For the person or business whose records are involved, the privacy or proprietary interest in that information should not change.* Nevertheless, because it is subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection. *See United States v. Miller*, 425 U.S. 435 (1976) (customer has no standing to contest disclosure of his bank records). Thus, [absent congressional action,] the information may be open to possible wrongful use and public disclosure by law enforcement authorities as well as unauthorized private parties. The provider of these services can do little under current law to resist unauthorized access to communications.

Title II of S. 2574 [i.e., the future Stored Communications Act] addresses access to stored wire and electronic communications and transactional records. It is modeled after the Right to Financial Privacy Act, 12 U.S.C. 3401 et seq. *to protect privacy interests in personal and proprietary information*, while protecting the Government's legitimate law enforcement needs.

S. Rep. No. 99-541 at 3 (1986) (emphasis added). *See also*, e.g., S. Hrg. 98-1266 at 17 (1984) ("In this rapidly developing area of communications which range from cellular non-wire telephone connections to microwave-fed computer terminals, distinctions such as [whether a participant to an electronic communication can claim a reasonable expectation of privacy] are not always clear or obvious.").

- a. Rule 41 Does Not Independently Require Probable Cause for the Compelled Disclosure of Stored CSLI.

As previously discussed, a Rule 41 warrant may be used to obtain stored CSLI from an ECSP under the SCA, as an alternative to a D Order. *See* 18 U.S.C. § 2703(c)(1). And, as will be discussed below, the Fourth Amendment may require the government to obtain a warrant when seeking CSLI. However, Rule 41 of the Federal Rules of Criminal Procedure, which specifies the procedures under which the courts may issue a warrant that satisfies the Fourth Amendment, nowhere affirmatively *requires* the government to seek such warrants. Rather, as Magistrate Judge Lenihan correctly describes, “Rule 41 of the Federal Rules of Criminal Procedure generally provides that the Government *may* secure a warrant upon a showing, consistent with the requirements of the Fourth Amendment, that there is probable cause.” *M.J. Order*, 534 F. Supp. 2d at 592. Indeed, Rule 41 primarily constrains not the government but the Court, by specifying that the Court “must” issue a warrant where probable cause has been demonstrated. Fed. R. Crim. P. 41(d)(1). Although the government ignores Rule 41’s procedures and thereby risks suppression of unconstitutionally seized evidence “at its peril” — see, e.g., *In the Matter of an Application of the United States for an Order Authorizing the Use of a Pen Register and a Trap And Trace Device*, 396 F. Supp. 2d 294, 324 (E.D.N.Y. 2005) — the Rule does not itself require the government seek warrants. It merely provides the procedure by which the government may do so.<sup>10</sup>

- b. The “Tracking Device Statute,” 18 U.S.C. § 3117, Does Not Independently Require Probable Cause for the Compelled Disclosure of Stored CSLI.

As the government notes, the purpose of 18 U.S.C. § 3117 — sometimes referred to as the “Tracking Device Statute” — is “to provide a court with extra-territorial jurisdiction over use

---

<sup>10</sup> The Judicial Conference Advisory Committee’s Notes to the 2006 Amendments to the Federal Rules of Criminal Procedure concerning tracking devices proves the point: “[w]arrants *may* be required to monitor tracking devices *when* they are used to monitor persons or property in areas where there is a reasonable expectation of privacy.” Quoted in *M.J. Order*, 534 F. Supp. 2d at 593 (emphasis added). Even assuming that obtaining stored CSLI constitutes “monitor[ing] [a] tracking device,” nothing in the Rule or in its notes affirmatively requires the government to obtain a warrant for such data.

of tracking devices installed within its jurisdiction.” Gov. Br. at 11. *See also id.* (“If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order *may* authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction.”) (emphasis added). This provision does not itself affirmatively require that the government obtain such a warrant or other order, or otherwise define the standards under which the use of a tracking device may be authorized. *See M.J. Order*, 534 F. Supp. 2d at 593, 595 (noting that the Tracking Device Statute does not specify the evidentiary standard applicable to the installation of a tracking device). *See also* S. Rep. 99-541 ) at 34 (noting that ECPA’s treatment of tracking devices “does not effect current legal standards for the issuance” of court orders for the installation of tracking devices).

c. The Wireless Communication and Public Safety Act Does Not Independently Require Probable Cause for the Compelled Disclosure of Stored CSLI.

The Wireless Communication and Public Safety Act of 1999 amended 47 U.S.C. § 222 to prohibit a phone company’s disclosure of “customer proprietary network information” (“CPNI”) — including “information that relates to the ... location ... [of] any customer of a telecommunications carrier ... that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship” — except “as required by law or with the approval of the customer.” 47 U.S.C. § 222(c)(1). With this minimal standard, Congress prohibited carriers from releasing location information on a solely voluntary basis. However, section 222 permits the disclosure of stored CSLI “as required by law,” including upon a less stringent showing required by, for example, civil discovery mechanisms. *See, e.g., ICG Communications, Inc. v. Allegiance Telecom*, 211 F.R.D. 610, 612 (N.D. Cal. 2002) (holding that CPNI may be disclosed under section 222(c)(1) in response to interrogatories and document requests). Section 222 does not contain any requirement that the government must obtain a warrant before obtaining stored CSLI, even when it reveals a customer’s location. *See generally* 47 U.S.C. § 222.

- d. CALEA's Restriction Against the Use of Pen Registers for Cell Phone Tracking Does Not Independently Require Probable Cause for the Compelled Disclosure of Stored CSLI.

As part of the Communications Assistance for Law Enforcement Act ("CALEA")<sup>11</sup>, Congress made it clear that the "Pen Register Statute" ("PRS") portion of ECPA,<sup>12</sup> which authorizes court orders allowing the government to install prospective "pen registers" and "trap and trace devices," cannot be used to authorize the acquisition of CSLI. *See* 47 U.S.C. § 1002(a)(1)(2). Specifically, in mandating that ECSPs make their facilities readily available to law enforcement for the acquisition of "call-identifying information" such as that collected by pen registers and trap and trace devices, Congress provided in CALEA that:

[W]ith regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number").

*Id.* However, as the government notes, it is not seeking to prospectively acquire CSLI such that the PRS would apply to its conduct, nor is it seeking an order under the PRS. Gov. Br. at 9-11. Nor does CALEA specify any other authority, such as Rule 41, that the government must rely on before acquiring such information; it only specifies that an order under the PRS alone will not suffice. *See* Gov. Br. at 9-11; 47 U.S.C. § 1002(a)(1)(2).

In sum, absent SCA protection, no other statute would require the government to demonstrate probable cause to a court before obtaining stored CSLI. Indeed, Section 2703's plain language protects not only stored CSLI but *all* information pertaining to a cell phone customer held by the cell phone provider: whether it's the *content* of a communication requiring a warrant under section (a), *subscriber information* like name and address requiring at least a subpoena under subsection (c)(2), or any "*other information*" requiring at least a D Order under subsection (c)(1).

---

<sup>11</sup> 47 U.S.C. §§ 1001-1010.

<sup>12</sup> 18 U.S.C. §§ 3121-27.

**B. The Stored Communications Act Permits the Court to Require a Probable Cause Warrant Rather than a D Order Prior to the Seizure of Stored CSLI.**

As Magistrate Judge Lenihan correctly held below, 18 U.S.C. § 2703(d) allows the Court to require the government to meet the requirements for the issuance of a Rule 41 warrant before ordering the disclosure of stored CSLI. While section 2703(d) articulates the minimum requirements for issuance of a D Order, it does not require a court to issue an order on such a showing. Rather, section 2703(d) creates a permissive standard that allows the Court in its discretion to deny the government's application for a D Order and instead require the government to seek a Rule 41 warrant pursuant to 18 U.S.C. § 2703(c)(1)(a). The statute provides the Court with the flexibility necessary in cases such as this one to accommodate novel privacy concerns and avoid serious constitutional questions.

**1. The Plain Language of 18 U.S.C. § 2703(d) is Permissive and Does Not Require Issuance of an Order Upon a Showing of Specific and Articulate Facts.**

The plain language of the Stored Communications Act, as well as its context within the ECPA statutory framework, supports Magistrate Judge Lenihan's conclusion that 18 U.S.C. § 2703(d) *permits* but does not *require* the Court to issue a D Order based solely on a showing of specific and articulable facts. Section 2703(d) reads:

A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and *shall issue only if* the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

18 U.S.C. § 2703(d) (emphasis added). As the Court noted below, “[Section 2703(d)] does not provide that such an Order shall issue ‘if’ or ‘whenever’ such a showing is made. Thus, under the plain language of the SCA, a showing of reasonable relevance is a *necessary*, but not necessarily *sufficient*, condition for issuance of an Order.” *M.J. Order*, 534 F. Supp. 2d at 608 (emphasis in original).

In sharp contrast to 18 U.S.C. § 2703(d)'s permissive language, Congress elsewhere in ECPA has provided for *mandatory* issuance of court orders based on a particular showing. *See*

*Tavarez v. Klingensmith*, 372 F.3d 188, 190 (3rd Cir. 2004) (the Court “must look to the surrounding words and provisions and their context.”). In particular, Title II of ECPA, the Pen Register Statute governing the installation of “pen register” and “trap and trace devices” that capture non-content communications routing information in real time, sets forth a mandatory standard under which courts must grant government applications for orders authorizing such surveillance:

Upon an application made under section 3122 (a)(1), the court *shall* enter an *ex parte* order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, *if* the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

18 U.S.C. § 3123(a)(1) (emphasis added). The PRS’ “shall...if” requirement stands in sharp contrast to the permissive “shall...*only* if” language found in 18 U.S.C. § 2703(d). If possible, the Court must ““give effect ... to every clause and word of a statute.”” *See Duncan v. Walker*, 533 U.S. 167, 174 (2001) (quoting *United States v. Menasche*, 348 U.S. 528, 538-39 (1955)). For the “only” in 18 U.S.C. § 2703(d) to have meaning, it must be construed to allow the Court the discretion to deny an application for a D Order even if a “specific and articulable facts” showing has been made. *See M.J. Order*, 534 F. Supp. 2d at 607-09. Not only is this the fair reading of Section 2703(d)’s plain language, which is all that is required to satisfy the doctrine of constitutional avoidance, *see infra* at subsection (2), it is the only plausible reading that gives the word “only” an effect.<sup>13</sup>

Recognizing the Court’s flexibility to impose additional requirements before issuing a D Order is consistent with Congress’ recognition that ECSPs were storing more (and more invasive) types of records and other information with uncertain protection under the Fourth Amendment.<sup>14</sup> As technology advances, not only do the quantity and quality of private records

---

<sup>13</sup> Notably, the permissive language of 18 U.S.C. § 2703(d) also stands in stark contrast to the language of Federal Rule of Criminal Procedure 41, which provides that the Court “*must*” issue a warrant if probable cause has been established. *Id.* at 41(d)(1).

<sup>14</sup> *See* note 10, *supra*.

stored by ECSPs grow, but the statutory distinction between types of information — e.g., between “contents” and non-contents — become increasingly uncertain. *See, e.g., In re Application of U.S. for an Order Authorizing use of A Pen Register and Trap On [XXX] Internet Service Account/User Name, [xxxxxxx@xxx.com]*, 396 F. Supp. 2d 45, 47-48 (D.Mass. 2005) (discussing difficulty of distinguishing content from non-content information as technology advances: “In the telephone world, it would seem easy to distinguish numbers dialed out and numbers dialed in from the contents of the communications which occur after the connection has been made.... In the internet world, it seems to me the problem is greater.”). Allowing disinterested magistrates the flexibility to require a greater showing from the government for the disclosure of particularly sensitive or novel types of private information ensures that the SCA’s protections are not made wholly obsolete by emerging technologies, consistent with Congress’ broad protective purpose.

Indeed, Congress in 1994 amended the SCA in CALEA to provide additional protections for transactional records other than basic subscriber information. *See* Pub. L. No. 103-414, Title II, § 207(a), 108 Stat. 4292 (Oct. 25, 1994). Prior to CALEA, any non-content information pertaining to an ECSP’s customer could be obtained not only with a mere subpoena. *See* Pub. L. No. 99-508, Title II, § 201, 100 Stat. 1861 (Oct. 21, 1986). CALEA, by specifically enumerating the limited subscriber information that could be obtained with only a subpoena under 18 U.S.C. § 2703(c)(2), created a new intermediate category of transactional information that could only be obtained using a warrant or a D Order. Congress did so because it recognized that “in the face of increasingly powerful and personally revealing technologies,” H.R. Rep. No. 103-827 at 13 (1994), the requirement of a mere subpoena was not sufficient to protect the privacy of the increasing quantity and quality of more invasive types of records threatening to reveal a “person’s entire on-line profile.” H.R. Rep. No. 103-827 at 17 (1994).

None of the legislative history cited by the government indicates that Congress intended to *require* rather than allow magistrates to issue D Orders based on the specific and articulable facts standard. The government points to Congress’ statements that “if a court order is sought



then the government must meet the procedural requirements of subsection (d)” (Gov. Br. at 18, quoting H.R. Rep. No. 99-647 (1986)) and that the specific and articulable facts standard is “an intermediate standard ... higher than a subpoena, but not a probable cause warrant,” (*id.* at 19, quoting H.R. Rep. No. 103-827 (1994) *reprinted in* 1994 U.S. Code Cong. & Admin. News 3489, 3511). Both of these statements are correct, yet neither indicates that the Court must issue a D Order when that standard is met, only that the government must meet that standard before the order may be issued. Instead, the legislative history cited by the government only demonstrates that meeting the intermediate standard is a *necessary* precondition for a D Order; it does not mean that such a showing will always be *sufficient* to obtain a D Order. To the extent the Court does not find that showing to be sufficient, it may deny the application and instead require the government to seek a Rule 41 warrant pursuant to 18 U.S.C. § 2703(c)(1)(a). As described below, considering the constitutional issues at play in this case, Magistrate Judge Lenihan was indeed *required* to do so by the doctrine of constitutional avoidance.

**2. The Doctrine of Constitutional Avoidance Requires That This Court Interpret 18 U.S.C. § 2703(d) as Permissive Because the Statute Otherwise Runs Afoul of the Fourth Amendment**

“‘[I]t is a cardinal principle’ of statutory interpretation ... that when an Act of Congress raises ‘a serious doubt’ as to its constitutionality, ‘this Court will first ascertain whether a construction of the statute is fairly possible by which the question may be avoided.’” *See, e.g., Zadvydas v. Davis*, 533 U.S. 678, 689 (2001) (quoting *Crowell v. Benson*, 285 U.S. 22, 62 (1932)); *Ashwander v. Tennessee Valley Authority*, 297 U.S. 288 (1936) (Brandeis, J., concurring) (“When the validity of an act of the Congress is drawn in question, and even if a serious doubt of Constitutionality is raised, it is a cardinal principle that this Court will first ascertain whether a construction of the statute is fairly possible by which the question may be avoided.”).

The doctrine of constitutional avoidance requires that section 2703(d) be interpreted as allowing Magistrate Judge Lenihan to deny the government’s application and require a Rule 41 warrant for stored CSLI, because that information may be — and, as described *infra*, is —



protected by the Fourth Amendment. If CSLI is constitutionally protected, a reading of 18 U.S.C. § 2703(d) that would require the Court to order such information's disclosure in violation of the Fourth Amendment would render that provision constitutionally suspect.

Magistrate Judge Lenihan properly avoided the serious question of whether the SCA violates the Fourth Amendment by allowing warrantless access to stored CSLI, which she and *amici* agree is protected by the Fourth Amendment. To avoid that question, she fairly read the SCA to permit, but not require, the issuance of a D Order based only on specific and articulable facts. This fair reading, supported by the statute's plain language, ensures that the SCA's protections will not be rendered unconstitutional as Fourth Amendment jurisprudence advances to protect new classes of ECSP-stored data — such as stored CSLI.

**C. The Fourth Amendment Protects Stored CSLI, Such That the Government Must Obtain a Rule 41 Warrant Rather Than a D Order Prior to its Seizure.**

The Government must obtain a Rule 41 warrant before seizing stored CSLI. The Fourth Amendment protects the location information of individuals in areas in which they have a reasonable expectation of privacy. *Karo*, 468 U.S. at 714-15. The Fourth Amendment also protects against warrantless searches of the person, including purses, pockets, briefcases and backpacks. *Hoffa v. United States*, 385 U.S. 293, 301 (1966). Inevitably, stored CSLI surveillance reveals an individual's location in a private space, as well as a cell phone's location in protected spaces, including on the person. Moreover, given the invasive nature of the records in question, stored CSLI can enable surveillance “dragnets” that courts have warned raise serious Fourth Amendment problems. Together, these factors require a Rule 41 warrant, as Magistrate Judge Lenihan demanded below.

**1. Stored CSLI Reveals Details about the Interior of Homes, Purses and Pockets, All Protected Spaces Under the Fourth Amendment.**

The Fourth Amendment protects against warrantless tracking of your physical location in a protected space. It also prohibits warrantless search of the person, including pockets and handbags. Stored CSLI enables both types of surveillance.

Two Supreme Court cases set forth the constitutional rule for tracking beepers officers place on vehicles and personal property. In *United States v. Knotts*, officers placed a transmitting beeper in a can of chemicals being transported in a car in order to aid surveillance of the vehicle while traveling on a public road. 460 U.S. at 278. The occupants of the car had no legitimate expectation that they would not be observed on the public road. First, there is a diminished expectation of privacy in a car.

One has a lesser expectation of privacy in a motor vehicle because its function is transportation, and it seldom serves as one's residence or as the repository of personal effects. A car has little capacity for escaping public scrutiny. It travels public thoroughfares where both its occupants and its contents are in plain view.

*Id.*, 460 U.S. at 281.

Further, travel in a car on public roads conveys location information to the general public. Police could have visually surveilled the car without violating the Fourth Amendment. The beeper merely allowed them to surveil more effectively. The Court stated that the Fourth Amendment does not impede the police from “augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.” *Id.* at 282.

Importantly, the Court emphasized that the surveillance in *Knotts* was narrow, and did not give the police any information about the presence of the chemicals in a home or other protected place. As the Court explained, “nothing in this record indicates that the beeper signal was received or relied upon after it had indicated that the drug . . . had ended its automotive journey at rest on respondent’s premises in rural Wisconsin.” *Id.* at 284-85. Because beeper surveillance gave location information for only a single car on a public road, the Court held that use of such a device was not a search.

*Knotts* relies on several questionable assumptions that courts should reconsider — and indeed which the Supreme Court has rejected in *Kyllo v. United States* — in light of modern technology and its impact on societal consensus about the expectation of privacy. See *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (“The question we confront today is what limits there are

upon this power of technology to shrink the realm of guaranteed privacy.”). *Knotts* equates mere visual surveillance with scientific enhancement of visual capabilities with a beeper. The observations are different in both quality and kind. Visual surveillance is time-consuming and difficult. Officers will not undertake it without some cause, regardless of the dictates of the Fourth Amendment. Technologically enhanced surveillance is cheaper and easier. In the case of CSLI, all the costs of collection and storage are borne by the cellular provider. Legal restrictions are the primary disincentives to the surveillance. The quality of the information is better. Visual surveillance does not enable officers to go back in time to find out where calls were made from. Accessing stored CSLI does. Visual surveillance is imperfect, technological tracking less so. *Knotts* is also objectionable because individuals do have some expectation of privacy on the public roads. People expect that they may get lost in a crowd, or be subject to fleeting observations, but not that they will be secretly and continuously tracked. *See, e.g.*, Wayne R. LaFare, *Search and Seizure: A Treatise on the Fourth Amendment* § 2.7(e) (4th ed. 2004). That is why we have anti-stalking laws.

The Supreme Court’s decision in *Kyllo* shows that Fourth Amendment jurisprudence has moved beyond these mistakes in *Knotts*. Technology can impact privacy and the law has critical role to play in maintaining the balance between liberty and enhanced government powers. *Kyllo*, 533 U.S. at 40 (holding that thermal imaging of heat waves emanating from the outside of a house is a search because court must “take the long view from the original meaning of the Fourth Amendment forward ... ‘in a manner which will conserve public interests as well as the interests and rights of individual citizens’” (citing *Carroll v. United States*, 267 U.S. 132, 149, (1925))).

As questionable as *Knotts* is, it is also limited to beeper tracking in public places of information the suspect voluntarily discloses to outsiders. But when use of a beeper allows police to infer facts about the inside of a home or other private space, a search takes place that requires a warrant. In *United States v. Karo*, the Court struck down the warrantless use of a beeper to track a canister of chemicals into a home. “Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests

in the home to escape entirely some sort of Fourth Amendment oversight.” 468 U.S. at 716. The *Karo* beeper allowed officers to learn something about the interior of a private space; *i.e.* that a can of chemicals was located there, so the surveillance was a search which required a warrant. *Id.* at 713. It did not matter that the information was not “intimate” or that the police could have guessed it by watching the chemicals enter the house from the public road. *Id.* at 715 (“Even if visual surveillance has revealed that the article to which the beeper is attached has entered the house, the later monitoring not only verifies the officers' observations but also establishes that the article remains on the premises.”). Taken together, *Knotts* and *Karo* stand for the proposition that there is a reasonable expectation of privacy in the presence of a person or object in a private place.

We cannot accept the Government's contention that it should be completely free from the constraints of the Fourth Amendment to determine by means of an electronic device, without a warrant and without probable cause or reasonable suspicion, whether a particular article — or a person, for that matter — is in an individual's home at a particular time. Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight.

*Id.* at 716.

Without a doubt, the government plans to use CSLI to learn whether suspects are in private places outside of public view. Stored CSLI is not too inaccurate to infer the location of individuals in private places. The government's reasons for seeking stored CSLI in this case are sealed. However, in Government's Exhibit D, a drug conspiracy case in which the government used stored CSLI, the information was used to “identify the locations used by targets of the investigation” as well as to “help link the defendants and to corroborate surveilling agent's observations by providing the general geographic area of the telephones.” Gov't Ex. D. Law enforcement uses the fact that the suspect's phone contacted the cell tower nearest his home to infer he is home, nearest the narcotic's kingpin's house to infer that they are together, nearest the drop off point to argue that he was present when the contraband was delivered. One can also imagine that the government can ask for all the numbers that made calls through the tower

nearest a political rally to infer that those callers attended the rally. The government quibbles with Magistrate Judge Lenihan's factual findings but does not promise that it does not and will not use the stored CSLI as evidence that calls are made from a constitutionally protected space or to infer facts about the interiors of private homes. Gov. Br. at 26.

Because CSLI can reveal constitutionally protected location information, it must be treated as Fourth Amendment protected, regardless of the mechanics by which the surveillance occurs. The Supreme Court rejects mechanical interpretations of the Fourth Amendment. *Kyllo*, 533 U.S. at 35. In *Kyllo*, the government used a "fairly primitive" thermal imaging device to detect heat radiating from the external surface of a house. *Id.* at 41 (J. Stevens dissenting). From the imaging, the government was able to infer details about the interior of the house, a constitutionally protected space. The Supreme Court rejected the government's view that because the heat waves were in the public domain, monitoring them was not a search: "We rejected such a mechanical interpretation of the Fourth Amendment in *Katz*, where the eavesdropping device picked up only sound waves that reached the exterior of the phone booth. Reversing that approach would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home." *Id.* at 35.

Regardless of where the target is located, warrantless cell phone tracking also allows law enforcement to illegally learn private facts about the contents of an individual's pocket or purse; that is, that the individual is carrying a cell phone. A pocket is protected under the Fourth Amendment. "When [an individual] puts something in his filing cabinet, in his desk drawer, or in his pocket, he has the right to know it will be secure from an unreasonable search or an unreasonable seizure." *Hoffa v. United States*, 385 U.S. 293, 301 (1966).

Electronic surveillance that gives police information about the contents of a pocket is a search as well. *Karo* held that the Fourth Amendment regulates electronic surveillance that allows officers to determine than an object is located somewhere that police would need a warrant to physically search. *Id.* at 719. Like the chemicals in *Karo*, electronic surveillance of a phone allows officers to learn not only that the target is inside a home, but also that the phone is

in a purse or pocket. The collection of stored CSLI will inevitably reveal that someone is carrying it, even though that information cannot be derived from visual surveillance, but only from a physical search of the person.

Imagine that a suspect, under visual surveillance, is seen holding the target phone as he enters his home. Inside the house, he gives the phone to his teenage daughter who is going to a sleepover, and she puts it in her pocket. She then drives to her friend's house across town. Once inside, she takes the phone out of her pocket and calls her father to say she arrived safely. It does not matter that the information might be of poor quality or quantity. "The Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained." *Kyllo*, 533 U.S. at 37-38 (finding that even if measuring heat emanating from a home did not reveal private information, "the detail of how warm — or even how relatively warm — *Kyllo* was heating his residence" was a search because these were details of the home). What matters is that, even if the government's assertion that cell tracking can only reveal the phone's "general vicinity," the government has still learned that the phone was removed from the home based on the daughter's call. That information was never revealed in public view and could only have been obtained by a physical search of the home, or the friend's home, or the daughter's pocket, subject to the Fourth Amendment. The same protections apply to tracking the phone electronically.

The government here argues that CSLI collected from the provider is not private, just as it argued that heat waves emanating from the walls of a home were not private. However, CSLI allows officers to infer information about the interior of a home or pocket, just as the imager allowed officers to learn about the house. While the quality of CSLI information may not be very good, just as the thermal imager in *Kyllo* was rather primitive, any information about the interior of a private space is protected, whether it is the presence of the phone in a pocket, the user in a home, or how warm someone decides to heat their home.

Empirical research shows that citizens strongly expect their location information is private and that they will not be tracked with their cellular phones unless and until law

enforcement demonstrates probable cause to a court. In “Research Report: A Supermajority of Californians Supports Limits on Law Enforcement Access to Cell Phone Location Information” by Jennifer King and Chris Jay Hoofnagle, the authors queried respondents about cell phone tracking. The survey asked, with respect to historical location data: “would you favor a law that required the police to convince a judge that a crime has been committed before obtaining location information from the cell phone company?” Seventy-three percent of respondents supported or strongly supported this requirement while 27% opposed or strongly opposed it. Jennifer King & Chris Jay Hoofnagle, *Research Report: A Supermajority of Californians Supports Limits on Law Enforcement Access to Cell Phone Location Information*, 8 (April 18, 2008), available at <http://ssrn.com/abstract=1137988>.

**2. The Invasive “Dragnet” Surveillance Enabled by CSLI Requires At Least A Probable Cause Showing.**

CSLI not only differs from the beeper surveillance allowed in *Knotts* in that it inevitably discloses information about pockets, purses and homes, but also because it enables dragnet surveillance. In isolation, the government’s application in this case does not appear to ask for dragnet surveillance. However, CSLI is ripe for such use. For example, law enforcement can use CSLI to discover the identity of every subscriber that connected to a particular tower in a defined time period, and then track those numbers back to find where the individuals came from and to where they traveled. It can use CSLI to determine location at any point in the past for as long as the cellular provider chooses to keep the information. It can use CSLI to track many, many people cheaply without taking up officer time. This kind of monitoring is quite different from a beeper placed in a can of chemicals to assist in visual surveillance of a particular drug conspiracy suspect. *Knotts*, 460 U.S. at 282.

The few courts to consider the problem of dragnet surveillance have agreed that it is one of the more difficult Fourth Amendment questions. In *Knotts*, the defendant challenged the tracking beepers on the grounds that “twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision.” *Id.* at 283. The Court rejected that

characterization of the beeper technology but did not disagree that mass surveillance technologies might raise a quite different and novel Fourth Amendment question. “If such dragnet type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.” *Id.* at 284. Similarly, in *United States v. Garcia*, 474 F.3d 994 (7th Cir. 2007), a case considering the tracking of a car with a global positioning system (“GPS”) device officers affixed to the carriage, Judge Posner opined that mass surveillance of vehicular movements with GPS devices raises important, difficult and novel Fourth Amendment issues:

New technologies enable, as the old (because of expense) do not, wholesale surveillance. One can imagine the police affixing GPS tracking devices to thousands of cars at random, recovering the devices, and using digital search techniques to identify suspicious driving patterns. One can even imagine a law requiring all new cars to come equipped with the device so that the government can keep track of all vehicular movement in the United States. It would be premature to rule that such a program of mass surveillance could not possibly raise a question under the Fourth Amendment—that it could not be a search because it would merely be an efficient alternative to hiring another 10 million police officers to tail every vehicle on the nation's roads. ...

Technological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive. Whether and what kind of restrictions should, in the name of the Constitution, be placed on such surveillance when used in routine criminal enforcement are momentous issues that fortunately we need not try to resolve in this case.

*Id.* at 998.

This Court need not resolve this difficult issue. Under the canon of constitutional avoidance, its existence requires that the SCA be interpreted to allow judges to demand probable cause before issuing warrants for location tracking. Further, the Court should categorically reject any rule that would allow access to stored CSLI without a Rule 41 warrant, in recognition of the fact that such surveillance applications, either alone or in aggregate, can rise to the level of an unconstitutional dragnet.



**3. Because a Reviewing Court Cannot Otherwise Ensure that The Disclosure of Stored CSLI Will Not Violate the Fourth Amendment, an Order Compelling the Disclosure of Such CSLI Should Only Issue If the Government Makes the Showing Required by Rule 41.**

An issuing Court cannot ensure in advance that the stored CSLI will not reveal information about a home, pocket or other private space. Unmonitored disclosure will inevitably reveal too much information. The Fourth Amendment problem only worsens as providers begin to keep more data, or when law enforcement asks for dragnet location information. Therefore, the government should be required to show probable cause before a court will compel the disclosure of stored CSLI.

A court can only protect a cell user's Fourth Amendment rights by requiring a warrant. Prior to granting a government petition for the disclosure of stored CSLI, courts are unable to ascertain that disclosure of such CSLI will not implicate individuals' reasonable expectation of privacy. In order to ensure that those rights are protected, the government must meet a probable cause standard before the Court grants its petition.

Agents seeking stored CSLI will have to show probable cause in every case, which is exactly what the Supreme Court approved of in *United States v. Karo*. In *Karo*, the government objected that

[i]f agents are required to obtain warrants prior to monitoring a beeper when it has been withdrawn from public view, . . . for all practical purposes they will be forced to obtain warrants in every case in which they seek to use a beeper, because they have no way of knowing in advance whether the beeper will be transmitting its signals from inside premises.

*Karo*, 468 U.S. at 718. The Supreme Court sharply rejected this view stating: "The argument that a warrant requirement would oblige the Government to obtain warrants in a large number of cases is hardly a compelling argument against the requirement." *Id.* Implicit in this response, of course, is that the Government should obtain a search warrant "in every case in which . . . they [do not] know[] in advance whether the beeper will be transmitting its signals from inside premises." *Id.* See also *id.* at 713 n.3 (given that law enforcement cannot know when a beeper has been withdrawn from public view, "warrants for the installation and monitoring of a beeper

will obviously be desirable since it may be useful, even critical, to monitor the beeper to determine that it is actually located in a place not open to visual surveillance”).

When tracking a cell phone through cell-site data, the Government will have no way of knowing in advance whether only public information will be revealed or whether private information will be discovered as well. While some monitoring will occur while the target is in a location visible from a public place, much of it will occur while the target is in a private home given a cell phone’s small size and portability. Because monitoring of a “beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment,” *id.* at 714, the Government must obtain a warrant before using cell-site data to track a target. *Id.* at 715-17.

Where officers cannot tell in advance whether surveillance will reveal intimate details, they must get a warrant first. In *Kyllo v. United States*, the Supreme Court required a warrant before law enforcement could use a thermal imager to scan a house. The government argued that it should not need a warrant for imaging that did not reveal “intimate details.” The Court rejected this proposal because it was not a “workable accommodation between the needs of law enforcement and the interests protected by the Fourth Amendment.” The courts cannot develop jurisprudence specifying what quality or quantity of information is “intimate” and even if it could: “[N]o police officer would be able to know in advance whether his through-the-wall surveillance picks up ‘intimate’ details-and thus would be unable to know in advance whether it is constitutional.” *Id.* at 39. Therefore, the Court required the government to get a warrant for any scanning of the home.

We have said that the Fourth Amendment draws ‘a firm line at the entrance to the house’. That line, we think, must be not only firm but also bright-which requires clear specification of those methods of surveillance that require a warrant. While it is certainly possible to conclude from the videotape of the thermal imaging that occurred in this case that no “significant” compromise of the homeowner’s privacy has occurred, we must take the long view, from the original meaning of the Fourth Amendment forward.”

*Id.* at 40 (citations omitted).

Post-disclosure remedies are utterly inadequate to protect constitutional rights. First, no after-the-fact remedy can adequately make up for a constitutional violation, never mind systemic

violations of fundamental rights. For example, when First Amendment rights are threatened, as with those under the Fourth, the law requires rigorous pre-disclosure court review. Post-disclosure remedies are by definition insufficient because requiring such disclosure destroys the First Amendment right at issue. *See, e.g., Doe v. Cahill*, 884 A.2d 451, 457 (Del. 2005) (“[S]etting the standard too low w[ould] chill potential [speakers] from exercising their First Amendment right to speak anonymously.”). *See also Highfields Capital Mgmt. L.P. v. Doe*, 385 F. Supp. 2d 969 (N.D. Cal. 2004); *Dendrite Intern., Inc. v. Doe No. 3*, 775 A.2d 756, 760-61 (N.J. Super. Ct. App Div. 2001). Reviewing courts must protect both the Fourth and the First Amendment rights at stake in location tracking before those rights are infringed.

Second, for the vast majority of people who are illegally tracked, but not charged, there is no practical remedy. CSLI tracking invades the rights of people who are not charged with an offense. These people have no remedy other than a Fourth Amendment claim for illegal tracking. *See* 18 U.S.C. § 2708 (permitting only civil suits against providers for knowing and intentional violations of the statute for non-constitutional violations). However, few if any lawyers are interested in taking on the expense of suing the government when ascertaining the monetary value of a privacy invasion is so difficult to determine. *See, e.g., In re Doubleclick Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 524-25 (S.D.N.Y. 2001) (noting that invasion of privacy losses are non-economic, not actionable under the Computer Fraud and Abuse Act). Additionally, statutory damages are set at \$1000, hardly worthwhile to an attorney considering whether to take on the burden of suing the government for violations of the Stored Communications Act. 18 U.S.C. § 2707(c) (“The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of \$1,000.”). Even those “fortunate” individuals who are charged with a crime as a result of illegal surveillance – and thus can move to suppress – may have no remedy for unlawful seizure of stored CSLI. *United States v. Leon*, 468 U.S. 897 (1984) (finding that the exclusionary rule is intended to deter illegal police conduct, not to cure the invasion of a

defendant's rights after it has already occurred, so there is no bar on using illegally seized information the police officers obtained in good faith). Rather, the magistrate judge is the party charged with protecting the defendant's rights before the search. *Id.* at 921 ("It is the magistrate's responsibility to determine whether the officer's allegations establish probable cause and, if so, to issue a warrant comporting in form with the requirements of the Fourth Amendment."). Courts abrogate this responsibility by allowing CSLI surveillance that may be unconstitutional. *See, e.g., In re: Application of the United States for an Order for Prospective Cell Site Location Information On a Certain Cellular Telephone*, 460 F. Supp. 2d 448, 462 (2006) ("At this point, however, the Court has no way of knowing if the government will use any cell site information it obtains in this manner. If it does, and information obtained leads to indictment, the issue can be litigated on a motion to suppress."). Magistrate Judge Lenihan, however, protected constitutional rights as the law envisions.

**4. CSLI is a Third Party Record in Which the Subscriber Has a Reasonable Expectation of Privacy.**

The government argues that there are no constitutional problems to avoid because stored CSLI is not protected by the Fourth Amendment under *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), which held that there is no reasonable expectation of privacy in either bank records or dialed telephone numbers. These cases do not support the government's position.

In *Miller*, the bank was the intended recipient of the financial records seized by the government. "When a person communicates information to a third party ... he cannot object if the third party conveys that information or records thereof to law enforcement authorities." *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984). However, the Fourth Amendment treats very differently revelations to the government by a party to the conversation and surveillance without the knowledge or consent of either party. *Karo*, 468 U.S. at 716 n.4, citing *United States v. White*, 401 U.S. 745, 749 (1971).

Nor is CSLI like phone numbers dialed in *Smith v. Maryland*. In *Smith*, the subscriber voluntarily gave numerical information to the telephone company so that his call could be connected.

[Smith] voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, [Smith] assumed the risk that the company would reveal to police the numbers he dialed. The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber. [Smith] concedes that, if he had placed his calls through an operator, he could claim no legitimate expectation of privacy. . . . We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.

*Smith* at 744-45 (internal citation omitted).

CSLI is not voluntarily given to the cellular provider by the subscriber, but generated by the provider itself as part of its provision of service. The caller does not know the location of the nearest cell tower. The tower information, however, is generated whenever the phone is on. The provider decides what historical tower call records to keep. The call commencement and termination records that are the subject of this particular request are generated not only when the subscriber calls, but also when someone calls the subscriber. CSLI is not necessarily generated by the subscriber, but by the caller. Unlike the numbers in *Smith*, which would have been given to a human operator, there is no latter day analogy for CSLI information that suggests that the phone user is knowingly and voluntarily conveying the information to the provider as part of a request for connecting a phone call.

While prior cell tracking decisions avoided resolving the Fourth Amendment issues, most courts agree that tracking individuals with their cell phones, whether prospective or historical, raises Fourth Amendment questions not resolved by *Smith v. Maryland*. See, e.g., *Orenstein II*, 396 F. Supp. 2d at 323 (“As in any tracking situation, it is impossible to know in advance whether the requested phone monitoring will invade the target’s Fourth Amendment rights. The mere possibility of such an invasion is sufficient to require the prudent prosecutor to seek a Rule 41 search warrant.”); *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747, 757 (S.D. Tex. 2005) ” (“Because the government

cannot demonstrate that cell site tracking could never under any circumstance implicate Fourth Amendment privacy rights, there is no reason to treat cell phone tracking differently from other forms of tracking under 18 U.S.C. §3117, which routinely require probable cause.”); *In re Application of U.S. for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System*, 402 F. Supp. 2d 597, 605 (D.M.D. 2005) (holding that the court will not enter an order authorizing disclosure of real time cell site information under authority other than Rule 41, nor upon a showing of less than probable cause.); *In re Application of U.S. for Orders Authorizing the Installation and Use of Pen Registers and Caller Identification Devices*, 416 F. Supp. 2d 390, 397 n.10 (D.Mass. 2005) (“[T]o the extent any new statute authorizing disclosure of prospective cell site information permitted warrantless tracking of a cell phone possessor in a private residence not open to visual surveillance, the court would need to assess its constitutionality under *United States v. Karo*.”) (citations omitted). *But see Stearns*, 509 F. Supp. 2d at 81 (distinguishing *Karo* and *Kyllo* by holding that Fourth Amendment doesn’t apply where there is “nothing presumptively illegal about the possession of a cellular phone” and distinguishing *Leon* by holding that the magistrate should leave the problem of constitutionality for the aggrieved defendant to litigate in a motion to suppress); *Gorenstein*, 405 F. Supp. 2d at 449-50 (applying *Smith v. Maryland*); *In re Application of U.S. for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; and (2) Authorizing Release of Subscriber Information and/or Cell Site Information*, 411 F. Supp. 2d 678, 682 (W.D. La. 2006) (finding the information sought not specific enough to allow the government to tell if the suspect is home, in the yard, or at his neighbor’s house so no Fourth Amendment problem).

Because CSLI allows law enforcement to track individuals and infer information it could not otherwise perceive about the interiors of homes and pockets, obtaining that information invokes Fourth Amendment protections. *Kyllo* controls, not *Smith*.

## VI. CONCLUSION

The Stored Communications Act provides a statutory floor of protection for information pertaining to the subscriber of a communications service, including stored CSLI, by requiring

that the government obtain at least a “specific and articulable facts” order under 18 U.S.C. § 2703(d) before obtaining such information from the service provider. However, the plain language of the statute, the legislative history and the doctrine of constitutional avoidance demonstrate that an issuing magistrate can and indeed must raise that floor and instead require the government to meet the warrant standard before authorizing the disclosure of stored CSLI, which reveals location information probably protected by the Fourth Amendment. For all the foregoing reasons, *amici* urge this Court to affirm Magistrate Judge Lenihan’s denial of the government’s application to obtain stored CSLI under 18 U.S.C. § 2703(d).

Respectfully submitted

Date July 31, 2008

By /s/  
Jennifer Granick, Esq.

Attorney for *Amicus Curiae* Electronic Frontier  
Foundation, *et al.*